Magic Quadrant pour les plates-formes de protection des terminaux

Publié le 31 décembre 2022 - ID G00752236 - 55 min de lecture

Par Peter Firstbrook , Chris Silva

Tous les fournisseurs de ce rapport proposent des solutions efficaces pour lutter contre mal intentionné attaques . Maintenant ce point final détection et réponse (EDR) est intégré dans PPE et évolution dans étendu détection et réponse (XDR), la principale considération pour la plupart acheteurs devrait être l'intégration avec sécurité opérations .

Hypothèses de planification stratégique

D'ici fin 2025, 80 % des organisations de type C sera acquérir point final détection et réponse (EDR) en tant que service de détection et de réponse (MDR).
D'ici fin 2025, plus de 50 % des organisations de type B sera consolider EDR en un _ portefeuille de fournisseurs de sécurité des investissements pour une sécurité plus efficace opérations .
D'ici fin 2026, 80 % des organisations de type A sera être consommation d'EDR dans le cadre d'un multitool étendu architecture de détection et de réponse (XDR).
Marché Définition /Description

Remarque : En raison d'une pause dans la couverture de tous les vendeurs par Gartner, il y a peut être vendeurs qui répondaient aux critères d'inclusion décrites mais non évaluées . _ Ces les fournisseurs ne sont pas inclus dans ce recherche .
Les plates-formes de protection des terminaux (EPP) permettent de déployer des agents ou des capteurs pour sécuriser géré terminaux , y compris les ordinateurs de bureau , les ordinateurs portables , les serveurs et les appareils mobiles.
Les EPP sont conçus pour prévenir une gamme de problèmes connus et inconnus. mal intentionné attaques . De plus, ils fournir la capacité d' enquêter et de remédier tout incident qui échapper aux contrôles de protection .
Le noyau Les capacités d'un EPP sont :

- Prévention et protection contre la sécurité menaces , y compris les logiciels malveillants qui utilisent des exploits basés sur des fichiers et sans fichier .
- La possibilité de contrôler (autoriser /bloquer) les scripts et les processus .
- La capacité de détecter et de prévenir des menaces en utilisant comportemental analyse de l'appareil données d'activité , d'application, d'identité et d'utilisateur.

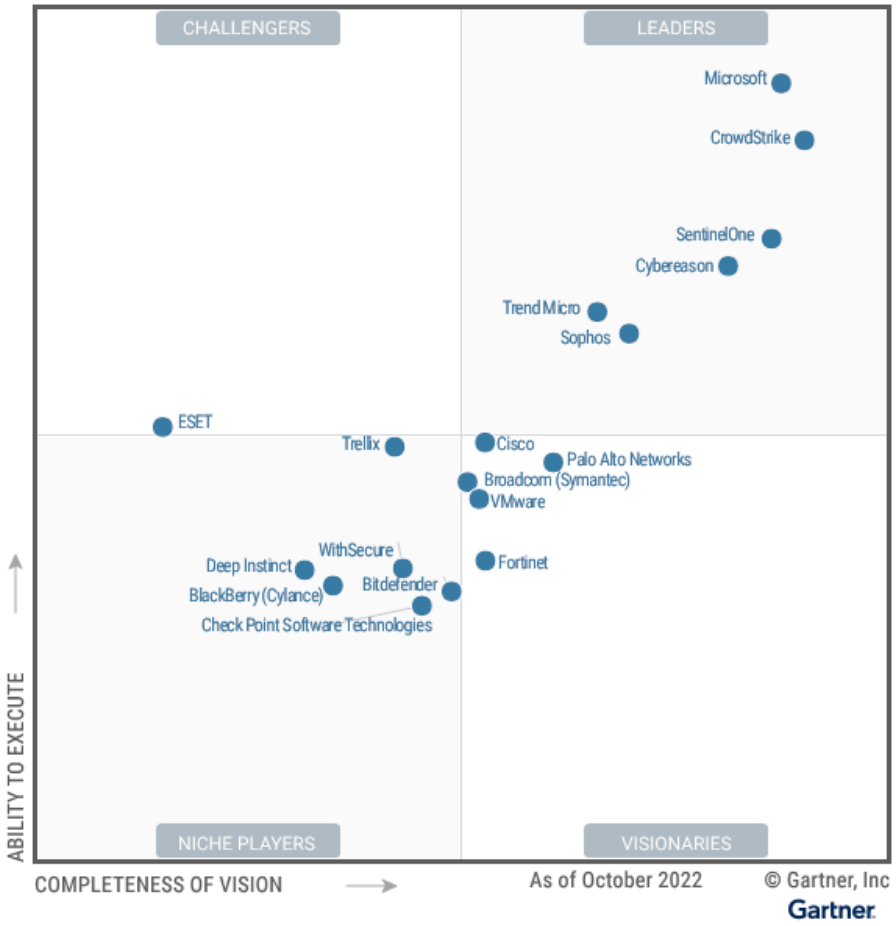
- Installations permettant d'enquêter plus avant sur les incidents et/ou d' obtenir des conseils pour y remédier lorsque les exploits échappent aux contrôles de protection .

Facultatif capacités souvent présents dans les PPE comprennent :

- Rapports de risque basés sur l'inventaire , la configuration et la gestion des politiques des terminaux .
- Gestion et rapport de l'état du contrôle de sécurité du système d'exploitation (OS) , tel que le disque paramètres de cryptage et de pare-feu local ou fonctionnalité de remplacement .
- Installations pour analyser les systèmes à la recherche de vulnérabilités et signaler ou gérer l'installation de correctifs de sécurité .
- Détection et réponse aux points finaux (EDR).
- Détection et réponse étendues (XDR).
- Services gérés .
- Compatibilité étendue du système d'exploitation avec les mobiles, les conteneurs, les instances virtuelles et les systèmes d'exploitation rares et en fin de vie .

Quadrant magique

Figure 1 : Magic Quadrant pour Endpoint Protection Platform



Source : Gartner (décembre 2022)

Fournisseur Points forts et précautions

Bitdefender

Bitdefender est un acteur de niche dans ce Magic Quadrant.
Bitdefender est un acteur de niche dans ce Magic Quadrant.
Son produit phare , la plateforme GravityZone , offre capacités EPP, EDR et maintenant XDR intégrées , qui sont gérées depuis le cloud. Tous les autres point final sécurité les produits sont fournis en tant que modules complémentaires .
Bitdefender aussi propose rapidement _ expansion géré service de détection et de réponse (MDR).
Bitdefender est le mieux adapté aux organisations de type B et C en Amérique du Nord et dans la région EMEA qui vouloir capacités de protection faciles à utiliser et efficaces .
Forces

- Bitdefender a une forte capacité de protection . C'est _ toujours parmi les plus performants dans les tests de protection contre les logiciels malveillants basés sur des fichiers et sans fichier .
- Bitdefender propose un agent modulaire pour les plates-formes physiques , virtuelles et cloud, qui est géré par une console SaaS pour toute l'administration de la sécurité des terminaux /serveurs . Il a également des offres complémentaire sécurité outils pour taille moyenne entreprises , filtrage des e-mails , protection du stockage , menace mobile défense (MTD), sandboxing de fichiers et gestion des vulnérabilités .
- Capacité EDR de Bitdefender est facile à utiliser, en partie grâce à d'excellents conseils et contextualisation à l'écran , tels que la cartographie MITRE ATT&CK. Les données sandbox et les sources de données externes sur la réputation des fichiers sont également bien intégré . automatique les actions de réponse facilitent efforts de remédiation .
- GravityZone XDR rassemble télémétrie à partir d'applications tierces , telles que les applications Microsoft Active Directory, Microsoft Office 365 et Amazon Web Services.

Précautions

- Sur l' axe Complétude de la vision, Bitdefender se classe pauvrement par rapport à certains concurrents pour sa stratégie marketing , qui est destiné à la taille moyenne entreprises .
- de Bitdefender marché partager et commercialiser partager croissance du marché EDR rester faible .
- Bien que Bitdefender dispose d'une capacité EDR facile à utiliser et d'une capacité XDR émergente (publiée au premier trimestre 2022), des

fonctionnalités avancées caractéristiques souhaitées par les grandes entreprises sont souvent manquant ou arrivé en retard .
- Le contrôle des applications et MTD ne sont pas disponibles sur la console cloud.

BlackBerry (Cylance)

BlackBerry (Cylance) est un acteur de niche dans ce Magic Quadrant.
La suite de produits EPP de BlackBerry comprend CylancePROTECT (EPP), CylanceOPTICS (EDR) et CylanceGUARD (MDR).
BlackBerry produit améliorations en 2022 se sont jusqu'à présent concentrés sur la simplification des enquêtes, les mappages MITRE ATT&CK et les politiques relatives aux données sensibles .
BlackBerry est une bonne option pour les organisations à la recherche de convergé point final la sécurité et la gestion, ainsi que celles à la recherche d'une suite de services MDR.
Forces

- Capacités XDR de BlackBerry étendu en 2022 grâce à un partenariat avec Exabeam et le lancement des services managés directs . Cela a permis l'intégration avec La solution de gestion des informations et des événements de sécurité (SIEM) Fusion d'Exabeam et accordée l'accès à d'autres produits et services intégrés avec pour une détection plus étendue .
- BlackBerry L'ensemble de produits Cylance Endpoint Security offre des outils de protection ce couvrent les terminaux PC , les serveurs et les appareils mobiles. BlackBerry intègre c'est CylancePROTECT et CylanceOPTICS des produits avec c'est unifié capacité de gestion des terminaux (UEM) pour opérationnaliser correction ou reconfiguration à grande échelle .
- En plus de MDR, BlackBerry propose une large gamme de services au sein de CylanceGUARD famille , y compris la réponse aux incidents , la sécurité évaluation et criminalistique analyse capacités ce étendre au-delà services centrés -EDR- gérés .
- BlackBerry a intégré continu authentification dans sa solution via le CylancePERSONA capacité , de détecter liés à l'identité menaces .

Précautions

- Après minimiser les plus connus Marque Cylance au profit de BlackBerry, la société a fait marche arrière et relancé le Cylance l'image de marque . Bien que ce c'est un bon coup, c'est est déroutant pour les clients potentiels .
- BlackBerry possibilité de vente croisée avec ses produits UEM pour gérer les PC et les appareils mobiles est tempéré par son petit marché part du marché UEM .

- Clients signalent toujours un niveau élevé de détections de faux positifs quand utilisant des versions de Cylance Endpoint Security antérieures à la version 3. Nous recommander que les clients mettent à niveau dès que possible.
- CylanceOPTICS a un faible global marché partager et bas CylancePROTECT taux d'attache . Récent amélioration des performances, basée sur les rôles contrôle d'accès et télémétrie optimisation et CylanceGUARD devrait toutefois contribuer à accélérer l'adoption de l'EDR de BlackBerry .

Broadcom (Symantec)

Broadcom (Symantec) est un visionnaire dans ce Magic Quadrant.
Son EPP principal est Symantec Endpoint Security Complete (SESC), qui inclut toutes les fonctionnalités EDR et XDR de la société .
Ce vendeur objectifs ses solutions dans de très grandes entreprises mondiales de type A et de type B ce veulent un portefeuille intégré de solutions de sécurité et à l'échelle de l'entreprise licence accords . Symantec récemment a lancé un nouveau programme pour mieux servir et soutenir les clients des petites et moyennes entreprises (PME) via des distributeurs locaux .
Broadcom récemment annoncé son intention d' acquérir l' encours actions de VMware. Au moment de l' évaluation , cependant , les deux Broadcom (Symantec) et VMware remplissaient les critères d'inclusion de ce Magic Quadrant et ont exploité séparément . Gartner va fournir un aperçu plus détaillé devient disponible sur la future feuille de route pour ces portefeuilles existants des fournisseurs .
Forces

- Broadcom (Symantec) réalise ses meilleurs scores dans ce Magic Quadrant pour l' échelle et la portée de ses opérations . Le SESC peut être déployé de manière hybride — qui est , en partie dans le cloud et en partie sur site . Il peut agréger les journaux et les alertes de l'un ou l'autre chantier de déploiement .
- Broadcom (Symantec) fournit une large gamme de composants EPP supplémentaires , notamment la défense Active Directory , le pare-feu personnel , le contrôle des appareils /applications et la sécurité des données . Certaines solutions aussi inclure protection complète des appareils mobiles .
- Produit de Broadcom (Symantec) bénéficie du nouveau introduit la protection adaptative, qui fournit automatisé et personnalisé restrictions d'exécution pour les comportements d'application abusifs employés dans des attaques « vivant de la terre » .
- Les accords d'entreprise peuvent réduire le coût d'un portefeuille de produits Broadcom (Symantec) .

Précautions

- Broadcom (Symantec) reçoit une note faible pour l'exécution marketing car il a réduit la taille de son canal de vente et s'est recentré ses efforts

exclusivement sur les plus grands entreprises . Bien que Symantec soit encore un important joueur au classement général marché , il est perdant marché partager et ses l'engagement client est à la traîne celui des chefs.

- Le score produit de Broadcom (Symantec) est abaissé par notre évaluation de ses résultats MITRE ATT&CK Phase 4 , qui étaient inférieur que la moyenne de ce Magic Quadrant.
- Broadcom (Symantec) reçoit de faibles scores pour l'innovation, en raison de son stratégie XDR limitée , au-delà intégration de la plate-forme XDR dans existant solutions d'entreprise SIEM/ d'orchestration de sécurité , d'automatisation et de réponse (SOAR).
- Le score de satisfaction client de Broadcom (Symantec) est dessous moyenne , avec des signaux très mitigés venant de différents segments de marché . Clients de Gartner souvent augmenter préoccupations concernant le support et le service de Symantec . Symantec plus grand entreprise clients paraissent plus satisfaits .

Check Point

Check Point Software Technologies est un acteur de niche dans ce Magic Quadrant. Check Point Harmony Endpoint assure la protection et la détection capacités , y compris l'apprentissage automatique (ML), comportemental analyse , bac à sable analyse et automatisation correction de détection menaces . Check Point Harmony Endpoint intègre avec Check Point Infinity pour les capacités XDR à travers Check Point point de terminaison , mobile, Internet des objets (IoT), réseau, e-mail et charge de travail cloud sécurité produits . La société récemment lancé tôt disponibilité d'Horizon XDR/XPR pour les réseaux, les points de terminaison , le cloud, la messagerie et l'IoT, et général disponibilité d'un service géré Horizon MDR/MPR . Horizon XDR/XPR n'a pas été évalué pour ce Magic Quadrant, mais être considéré pour évaluation dans le prochain édition .
Le point de contrôle est présent dans le monde entier régional marchés . C'est les produits conviennent à tous les types d' organisations , en particulier ceux qui sont des clients Check Point existants .
Forces

- Check Point obtient de bons résultats pour le marché compréhension et produits , comme son large gamme d' intégrés sécurité des produits fournit possibilités de consolidation et d'intégration pour simplifier opérations et sécurité .
- Check Point Harmony Endpoint inclut une grande variété de technologies de protection non standard , telles qu'un pare-feu personnel natif (non-OS) , le contrôle du port USB, la perte de données (DLP), le chiffrement , la protection contre le phishing des e-mails, le désarmement et la reconstruction du contenu, et le navigateur d'entreprise Harmony Endpoint .

- Check Point Harmony Endpoint également couvre les systèmes d'exploitation mobiles , tels qu'Android et iOS, dans le cadre d'une solution intégrée .
- Check Point obtient un score élevé pour le client expérience . Il met l'accent facilité d'utilisation pour la sécurité moins mature organisations , avec caractéristiques comme automatisé _ analyse de l' attentat à chaîne , automatisé correction et prédéfinis recherches communes _ menaces , telles que la vulnérabilité Log4j et le type d' attaque auquel Vents solaires clients abattre victime .

Précautions

- Check Point pour la capacité d' exécution sont réduits par son pauvre marché réactivité , comme en témoigne la faible niveaux du marché EPP pénétration et esprit partager , malgré disposant des ressources d'un grand groupe respecté sécurité vendeur .
- Check Point n'a pas développé le flux de travail EDR approfondi et les playbooks personnalisés ou comportementaux règles ce serait appel aux organisations avec de grands et complexes sécurité centres d'opérations (SOC).
- Capacité EDR de Check Point serait bénéficier de conseils et d'une automatisation plus prescriptifs en matière de remédiation .
- Check Point Harmony Endpoint a une « empreinte » plus importante que de nombreuses solutions, tant en termes de mémoire que de nombre de services et de processus utilisé lorsque tous les composants sont installés . Le point de contrôle est investir dans la réduction de l' empreinte Harmony Endpoint .

Cisco

Cisco est un visionnaire dans ce Magic Quadrant.
Cisco Secure Endpoint se décline en trois niveaux — Essentials, Advantage et Premier — dont chacun ajoute plus d'EDR et de chasse aux menaces capacité . Le point de terminaison sécurisé est intégré avec l' autre réseau Cisco et identité sécurité produits dans Cisco SecureX , une plate-forme XDR native du cloud fournie sans frais supplémentaires . Début 2022 , Cisco a lancé Cisco Secure Endpoint Pro, un service qui fournit une assistance téléphonique , des playbooks et des enquêtes définies directement du Cisco Talos Intelligence Group.
Cisco se concentre sur les marchés nord-américain et EMEA , mais il est aussi présent en Asie/Pacifique et au Japon, et en Amérique du Sud. La plupart des clients de Cisco sont des entreprises de type A ou de type B.
Forces

- Cisco obtient de bons résultats en matière de stratégie marketing et d'exécution . C'est le succès à cet égard est reflète dans sa fort marché partager .

- de Cisco les scores de produit et d'innovation bénéficient de Cisco SecureX , une plate-forme XDR qui unifie la sécurité de Cisco capacités avec gestion de cas inter- produits , recherche , investigation et correction capacités .
- En 2021, Cisco a acquis Kenna Security, qui fournit basé sur le risque gestion des vulnérabilités pour aider à hiérarchiser patcher .
- Cisco obtient de bons résultats pour ses géographique stratégie , en raison d' un canal mondial étendu programmes de partenariat , de service et d'assistance à travers régions et langues , ainsi que ses vastes ressources de formation .

Précautions

- Cisco Secure Endpoint ne fournit pas de pare-feu personnel natif ni de sécurité des données capacité .
- Cisco de produits EDR, Security Service Edge (SSE) et Secure Email Gateway (SEG) est intégré par Cisco SecureX pour la réponse aux incidents , mais les consoles de gestion et la politique l'intégration fait défaut .
- Correction EDR manuelle capacités , telles que la télécommande shell , ne sont pas disponibles depuis la console SecureX .
- Cisco SecureX ne stocke pas les données de journal de manière centralisée , mais récupère les données à la demande à partir d'autres magasins de journaux. La recherche avancée orbitale a une interface différente de Cisco Secure Endpoint ou SecureX .

CrowdStrike

CrowdSrike est un Leader dans ce Magic Quadrant.
La plateforme CrowdStrike Falcon maintenant comprend un ensemble complet de CrowdStrike posséder intégrations , y compris ceux pour la protection de l'identité , la sécurité du cloud et la surveillance de l'intégrité des fichiers . Ces s'asseoir aux côtés de l' EDR existant , des services gérés et des extras comme le contrôle des appareils , la gestion des pare-feu, la gestion des vulnérabilités et les correctifs .
En 2021, CrowdStrike acquis Humio , un fournisseur de solutions SIEM, pour créer des intégrations XDR dans la console Falcon. Humio technologie est maintenant la base de CrowdStrike Falcon LogScale , qui peut être utilisé à long terme _ possibilité de stockage . De plus, CrowdStrike récemment acquis Reposify , qui fournit externe capacités de gestion de la surface d'attaque (EASM) . CrowdStrike a également a créé la CrowdXDR Alliance et elle participe à l'Open Cybersecurity Schema Framework (OCSF) , qui viser à développer intégrations prêtes à l'emploi plus approfondies avec tôt partenaires .
FouleStrike rivalise à l'échelle mondiale , mais ses le plus grand base installée est en Amérique du Nord. C'est les produits conviennent aux organisations de type A et de type B . Il a également des offres services gérés adaptés aux organisations de type C .
Forces

- CrowdStrike les scores les plus élevés sont pour le marché compréhension et innovation. Ces attributs se reflètent dans la vaste portée de ses offrande , qui maintenant comprend un ensemble croissant de fonctionnalités de protection des charges de travail dans le cloud et de surveillance des conteneurs/ sans serveur , ainsi qu'une prise en charge complète des charges de travail traditionnelles des serveurs .
- CrowdStrike obtient des scores constants fortement pour le client l'expérience , l'innovation et l'ensemble viabilité . Il a continué à fonctionner Bien en 2022, malgré fort la concurrence des nouveaux entrants dans le quadrant Leaders.
- CrowdStrike continue de livrer c'est propres services MDR et de réponse aux incidents à un grand pourcentage de ses clients et partenaires MDR .
- L'acquisition d' Humio fournit FouleStrike avec une base solide pour l'expansion XDR.

Précautions

- CrowdStrike obtient de mauvais résultats pour son tarification . C'est liste les prix sont généralement plus haut que la moyenne des fournisseurs de ce Magic Quadrant, et ses remises plus petites , bien que nous le voyons prix plus agressif en 2022.
- de CrowdStrike dans ce Magic Quadrant prend compte de ses résultats de test MITRE ATT&CK phase 4 2022 , qui montrent moins couverture tactique et technique que autre fournisseurs dans ce Magic Quadrant.
- FouleStrike ne fournit pas d' option de gestion sur site pour les réseaux « à espacement aérien » ou à faible bande passante. environnements . Ni fait il prend en charge les systèmes d'exploitation Microsoft Windows Server 2003 ou Windows XP .
- CrowdStrike L'approche XDR est immature, par rapport aux approches XDR des autres leaders de ce Magic Quadrant.

Cybereason

Cybereason est un Leader dans ce Magic Quadrant.
Cyberaison propose une solution cloud-native, la Cybereason Plate-forme de défense , avec des capacités EPP, EDR et MTD . En 2022, Cybereason en partenariat avec Google pour intégrer c'est moteur d'analyse avec les capacités SIEM/SOAR back-end des solutions de Google . Il a fait cela pour permettre les déploiements XDR et les capacités de criminalistique numérique et de réponse aux incidents (DFIR) qui aident à automatiser les enquêtes.
La solution de Cybereason est disponibles à partir du cloud, et pour des applications sur site ou hybrides déploiement . La société offre MDR à la fois directement et à travers partenaires , avec l' inclusion de plate - forme pour MDR s'étendant aux systèmes d' exploitation mobiles .
Cyberaison cibles principalement EMEA, Japon et Amérique du Nord. Sa solution est convient aux organisations de type A et B . De plus , Cybereason les services gérés

font attrayant pour les organisations de type C cherche à externaliser les opérations EDR .
Forces

- Cyberaison présentation des données sur les menaces , à l'aide c'est MalOp événement catégorisation pour guider la chasse aux menaces activité , peut être utile aux organisations novices en matière d'EDR et de menace la chasse .
- Cyberaison des offres large couverture du système d'exploitation , y compris les systèmes d'exploitation mobiles . Il offre contrôle des périphériques pour gérer les supports amovibles , l'isolation des périphériques (escrocs) et la prise en charge du pare-feu personnel sur les systèmes d'exploitation , y compris Linux. L'offre Cloud Workload Protection de Cybereason offre une protection pour conteneurisé charges de travail et spécifiques détection et réponse capacités pour conteneurisé espaces de travail .
- Cyberaison des offres large couverture de la plate-forme . Il complète ce avec la possibilité d'examiner le trafic réseau pour détecter d'éventuels indicateurs d' attaque (IOA), analyse des e-mails et prise en charge des patcher .
- Quelques les options de correction sont automatiquement créé et peut être lancé à partir de la console pour adresser toutes les machines concernées . Les corrections manuelles sont assistées par une télécommande coquille . Des actions de triage rapides, telles que le processus de mise à mort , la mise en quarantaine et l'isolement , peuvent être pris manuel ou automatisé .

Précautions

- Cyberaison Le score Capacité d' exécution est publiquement _ _ signalé recrutement réductions ce a eu lieu en octobre 2022.
- Cyberaison manque d'une large gamme d' outils au-delà ceux axé sur les points finaux . Par exemple , il manque de produits SEG, SSE, NDR et de protection des données .
- de Cybereason pour la géographie stratégie est abaissé par son limité prise en charge linguistique (uniquement anglais et japonais).
- L' architecture de l'agent Cybereason installe un grand nombre de processus qui utilisent une quantité considérable quantité de mémoire.

Deep Instinct

Deep Instinct est un acteur de niche dans ce Magic Quadrant.
Deep Instinct est un privé entreprise basé en Israël et aux États- Unis les clients se trouvent principalement en Amérique du Nord, en Europe et au Japon.
Deep Instinct a développé une profonde cadre d'apprentissage (DL) pour automatiquement prévenir fichiers et comportements malveillants . L' entreprise se concentre sur l'exploitation son expertise DL pour fournir protection autonome et automatisée sans analyste implication .

Deep Instinct pour Endpoint est adapté aux organisations à la recherche d'un compagnon EPP basé sur DL pour les outils EDR ou pour des cas d'utilisation plus isolés (avec une bande passante limitée ou un air gap) et automatisés .
Forces

- Deep Instinct obtient des scores élevés en matière d'innovation en raison de son approche DL de la prévention , avec une capacité EDR légère . Comportemental détection mécanismes résident sur le point de terminaison , qui réduit dépendance à la connectivité Internet et aux mises à jour fréquentes .
- DL est une variante des algorithmes ML . Il utilise plusieurs couches pour résoudre les problèmes en extrayant connaissances à partir de données brutes et transformant ça à chaque niveau , souvent surperformant techniques traditionnelles de ML.
- Récent améliorations de Deep Instinct produit inclure la classification du cadre MITRE ATT&CK des éléments détectés menaces , réputation analysis , un moteur comportemental « EDR-lite » pour la attaques et correction de la restauration du registre .
- Deep Instinct fournit un modèle PowerShell DL dédié pour détecter scripts PowerShell malveillants .

Précautions

- Instinct profond la note du produit est réduit par son le produit se concentre uniquement sur la prévention , par opposition à la détection et à la réponse . Sa capacité EDR est contraint . Il n'a pas de détails journaux d'événements . Menace chasse , comportement personnalisé règles et avancées remédiation les fonctionnalités sont limitées .
- Deep Instinct fournit uniquement la prévention des logiciels malveillants . Il n'offre pas _ n'importe quel supplémentaire point final sécurité , telles qu'un pare -feu personnel , le contrôle des ports et des périphériques , ou la sécurité des données , telle que le cryptage . Ni fait il fournir un large portefeuille de sécurité des infrastructures contrôles .
- Les résultats des tests publics d'AV-TEST, SE Labs et MITRE, qui utilisent des échantillons de logiciels malveillants connus , ne peuvent pas démontrer que propose Deep Instinct substantiel amélioration de la précision par rapport aux autres méthodes de protection contre les logiciels malveillants.
- Pour les très grandes entreprises , les capacités de gestion de Deep Instinct , telles que l'administration basée sur les rôles , sont limitées , avec localisation uniquement dans les consoles de gestion en anglais et en japonais . C'est produit prend en charge la plupart des systèmes d'exploitation Windows , y compris embarqué ceux , mais offre seul prise en charge limitée de macOS et Linux. Deep Instinct n'a pas investi dans la charge de travail cloud capacités au-delà prévention .

ESET.

ESET est une entreprise privée possédé slovaque entreprise avec 30 ans d' expérience dans l' industrie du PPE et un savoir-faire reconnu laboratoire de recherche . Depuis le précédent édition de ce Magic Quadrant, ESET a lancé son module cloud EDR sur sa plateforme PROTECT Cloud, et la protection Docker. La société aussi offre un bac à sable de logiciels malveillants et des flux de renseignements sur les menaces , y compris de nouveaux rapports avancés sur les menaces persistantes (APT).
Appels ESET principalement aux organisations de type B et de type C de taille moyenne dans les pays qu'elle prend en charge, principalement dans la région EMEA et en Amérique du Nord.
Forces

- L'un des meilleurs scores d'ESET est pour le produit capacité . ESET fait bien dans les tests publics anti-malware et de performance. Il a été l'un des premiers à adopter les techniques de ML. Récent améliorations incluent une protection contre les attaques par force brute du réseau pour les exploits des protocoles RDP (Remote Desktop Protocol), FTP et Server Message Block (SMB), et des améliorations de l' analyse et du traitement des scripts.
- Pour l'entreprise clients ce exiger , ESET fournit une architecture de déploiement pour les systèmes à espacement aérien .
- ESET obtient de bons résultats pour sa opérations capacité . La console de gestion ESET est disponible en 23 langues , ce qui fait du c'est un bon choix pour le monde distribué entreprises et entreprises ce exiger régional localisation .
- ESET a introduit le MDR et les services de mise en œuvre directement dans certains pays et via le canal partenaires dans d'autres .

Précautions

- ESET obtient de mauvais résultats pour le marché la compréhension et l'innovation, car il en retard derrière concurrents dans le déploiement de fonctionnalités innovantes tels que la livraison dans le cloud , l'EDR, le MDR direct et le XDR.
- Bien qu'ESET fasse bien dans les tests de prévention publique , ses résultats de test MITRE ATT&CK Phase 4 montrent moins de niveau technique détections et indiquent la nécessité d'une plus grande que nombre moyen de changements de configuration.
- ESET n'a pas participé à la partie Linux des derniers tests MITRE ATT&CK, car il ne supportait pas Linux au moment de l'évaluation Cependant , il introduit le support EDR Linux au premier trimestre 2022.
- ESET les scores des produits sont affaiblis par un manque de capacités EDR avancées et de capacités tels que la gestion des vulnérabilités et la gestion de la configuration pour durcir endpoints (prévus au premier semestre 2023).

Fortinet

Fortinet est un visionnaire dans ce Magic Quadrant.
Fortinet s'est concentré ses efforts d'innovation pour introduire davantage d'intelligence artificielle (IA) - enquête formée , automatisée correction et prise en charge des règles personnalisées , et sur l'amélioration de l' intégration de la sécurité tierce des produits dans la console FortiXDR .
FortiXDR combine Fortinet endpoint , sécurité IoT , sécurité du réseau, de la messagerie, de l'identité et du cloud capacités , ainsi que l'infrastructure réseau, en une seule solution holistique . FortiEDR peut déclencher des actions de remédiation à travers infrastructure tierce , y compris les pare-feu et l'infrastructure d'accès au réseau Zero Trust .
Fortinet a une portée mondiale . C'est les produits sont bien adaptés aux organisations à la recherche d'une plate-forme de sécurité XDR intégrée .
Forces

- FortiXDR des offres large l'intégration capacité et règles automatisées et personnalisées . Son EDR fournit télécommande coquille accès au manuel remédiation .
- Fortinet peut intégrer avec plusieurs lacs de données et SIEM tiers et analyse de données outils , permettant l'ingestion à partir d' ensembles de données cloud et tiers pour l'analyse des données sur les menaces .
- Fortinet maintient faible Ressource utilisation et prise en charge étendue du système d'exploitation, malgré l'ajout de nouvelles fonctionnalités de logique et d'agent . C'est Ressource utilisation est de manière louable faible , en comparaison avec solutions concurrentes .
- Les résultats des tests MITRE ATT&CK de FortiEDR ont grandement amélioré en 2022.

Précautions

- Fortinet obtient de mauvais résultats en matière d'exécution marketing . Celui de la société marché partager et penser partager parmi les acheteurs EDR et XDR restes bas , au-delà c'est sécurité du réseau existant clients .
- Fortinet ne fournit pas de solution intégrée capacité pour MTD sur les appareils mobiles, contrairement aux fournisseurs avec concurrents et comparables des solutions tarifées .
- Bien que Fortinet ait son posséder services gérés , adoption de ceux-ci est faible , comparé avec services concurrents d' autres vendeurs .
- Fortinet prévoit de retirer la possibilité d'héberger son gestionnaire central sur site en mode hors ligne pour les environnements . Par conséquent , à l'avenir, tous les déploiements sera nécessitent une connexion Internet à partir du gestionnaire central FortiEDR .

Microsoft

Microsoft est un leader dans ce Magic Quadrant.
Microsoft propose une collection de fonctionnalités EPP/EDR de marque Defender à travers deux niveaux de licence dans son offre Defender for Endpoint . L'antivirus Microsoft Defender de base est inclus avec les licences de système d'exploitation Windows . Gestion des menaces et des vulnérabilités , réduction de la surface d'attaque , EDR et une augmentation gamme de services gérés directs sont disponibles dans divers options de licence .
Microsoft est expansion c'est sécurité capacités pour macOS , Linux et les systèmes d'exploitation mobiles , ainsi que des solutions pour les appareils IoT. Le centre de sécurité Microsoft Defender fournit une capacité XDR prête à l'emploi à travers Microsoft sécurité produits (EPP/EDR, SEG, accès cloud courtier en sécurité , IoT et Active Directory) terminé avec automatique actions de livre de paie . Les solutions Sentinel SIEM/SOAR de Microsoft peuvent étendre le flux de travail du centre de sécurité grâce à l'intégration avec fournisseurs tiers . _ Les solutions Sentinel et Defender for Endpoint bénéficient de l'intégration avec UEM de Microsoft et de la fonctionnalité Azure .
Microsoft Defender pour Endpoint convient aux organisations de type A, B et C dans toutes les régions .
Forces

- Microsoft les scores les plus élevés sont pour ses marché compréhension et dans l'ensemble viabilité . Cela en partie reflète la bonne performance de son entreprise de sécurité . Il a également reflète un mouvement précoce pour définir et faire évoluer la catégorie émergente XDR , avec profond l'intégration et l'automatisation entre Microsoft Defender pour Endpoint et d'autres produits Microsoft , en particulier Azure Active Directory, qui permet une émergence identité menace capacité de détection et de réponse (ITDR) .
- La gestion de la surface d'attaque externe de Microsoft Defender est maintenant en général disponible , ce qui permet de mieux gestion des vulnérabilités .
- Microsoft fournit stockage de bûches généreux conservation par défaut, et inclut le contrôle de la navigation Web , le contrôle des appareils et la protection du réseau. Autre vendeurs facturent souvent séparément pour ces les choses .
- Des partenariats avec , par exemple , AttackIQ et Illusive , et l' intégration open log capacité de Microsoft Sentinel étendre l'intégration au-delà uniquement des produits Microsoft .

Précautions

- Microsoft propose nombreux variations et permutations de licence et de conditionnement qui inclure Defender pour la sécurité des terminaux capacités . Les acheteurs doivent s'assurer ils obtenir uniquement les produits et

fonctionnalités ils besoin , ou combiner leurs budgets avec ceux des autres d'entreprise acheteurs pour acquérir des portefeuilles plus larges de logiciels de sécurité et de collaboration.

- Microsoft fournit seul soutien limité pour les personnes âgées OS . Aussi , là n'est pas possible d'héberger sa solution Defender for Endpoint sur site ou de gérer efficacement les systèmes qui ne se connectent pas à Internet.
- Microsoft Defender pour Endpoint est un complexe outil de menace chasse et surveillance proactive avancée . Cela peut ne pas convenir aux organisations sans expérimenté sécurité personnel d'exploitation ou géré partenaires fournisseurs de services de sécurité (MSSP) .
- Microsoft Defender Experts n'est pas un service MDR complet. De plus , bien que Microsoft ait annoncé Microsoft Security Experts, un service MDR, plus tôt en 2022, il était disponible uniquement en avant-première publique au moment de l'analyse .

Palo Alto Networks

Palo Alto Networks est un visionnaire dans ce Magic Quadrant.
Sa plate-forme Cortex XDR combine la protection et la détection des terminaux , du réseau et du cloud capacités , ainsi que des intégrations avec la société un portefeuille d'infrastructures plus large et des fournisseurs de sécurité tiers . Cortex XDR n'est pas disponible en version sur site ou auto- hébergée . Le service MDR de l'unité 42 de Palo Alto Networks a été publiquement lancé le 3 août 2022 ; il des offres géré menace recherche et prend en charge la mise en œuvre initiale et le réglage de l' outil EDR de l'entreprise .
Palo Alto Networks est approprié pour les organisations de type A et de type B avec actifs critiques qui nécessitent une détection et une défense de la couche réseau .
Forces

- Palo Alto Networks obtient un score élevé en matière d'innovation grâce à l'introduction des capacités XDR sur sa plate-forme Cortex XDR. La plate-forme Cortex XDR reçoit mises à jour hebdomadaires de son ML, qui sont livrées efficacement et peut exporter des données vers des outils de gestion de journaux tiers .
- Palo Alto Networks obtient un score élevé pour la nature étendue de ses offrande , qui comprend une combinaison de réseau, de cloud et de point de terminaison des technologies de détection adaptées aux clients avec existant investissements dans ses solutions.
- Palo Alto Networks a joué bien dans les deux tests AV-Comparatives 2021 et dans les évaluations MITRE ATT&CK Phase 4 en 2022.
- Le PPE de Palo Alto Networks est vendu en huit régions du monde. Parmi les vendeurs évalué dans ce Magic Quadrant, Palo Alto Networks offre le troisième plus grand nombre d'emplacements d'hébergement cloud .

Précautions

- Palo Alto Networks reçoit une note faible pour le marché réactivité , grâce à sa faible part de marché du PPE .
- Bien que Palo Alto Networks offre les services gérés , tels que les services gérés menace la chasse , l'adoption est limité (données d'adoption pour les nouveaux le service MDR lancé n'était pas disponible pour l'évaluation).
- Bien que les scores de satisfaction client de Palo Alto Networks sur la plateforme Peer Insights de Gartner soient comparables à ceux des autres fournisseurs dans ce Magic Quadrant, il a des scores inférieurs à la moyenne pour la facilité d' intégration avec des API et des outils standards .
- Palo Alto Networks n'a pas participé aux tests de l'industrie macOS et Microsoft Windows menés par AV-TEST en 2022.

SentinelleOne

SentinelleOne est un Leader dans ce Magic Quadrant.
SentinelleOne fournit des capacités EDR et XDR pour répondre aux besoins et aux budgets d'un large éventail de clients. Il a également des offres c'est posséder services managés et partenaires avec premier fournisseurs de MDR tiers . En 2021, SentinelOne acquis Scalyr , un fournisseur de solutions de journalisation de sécurité et de gestion des événements , pour fournir la base de son expansion XDR . De plus , en mai 2022, SentinelOne acquis Attivo Networks pour ses capacités IDTR et sa tromperie caractéristiques .
Les principaux marchés de SentinelOne sont l'Amérique du Nord et l'EMEA, mais cette fournisseur a également une présence importante au Moyen-Orient. Il propose des options de service d'assistance adaptées à tous les types d'organisations dans chacun de ces domaines . régions .
Forces

- SentinelOne continue d'étendre sa portefeuille de produits basé sur les acquisitions. Notamment , il est apportant c'est Singularité Identité, Singularité Ranger AD et Singularité Hologramme tromperie offres à commercialiser en tant que composants de plate-forme.
- SentinelOne a continué d'étendre son réseau de partenaires MDR et a constaté le taux d'attachement de ses posséder les services gérés augmentent dans le passé année .
- en charge des systèmes d' exploitation Windows hérités , du macOS d'Apple et de nombreuses versions de Linux est un force . SentinelleUn prend rapidement en charge les derniers chipsets et systèmes d'exploitation Apple dès leur lancement .
- SentinelleOne obtenu d'excellents résultats dans les évaluations MITRE ATT&CK Phase 4 du premier trimestre 2022. Cela réaffirme c'est capacité à détecter toutes les attaques et à fournir tous les détails sur les techniques et les tactiques utilisé .

Précautions

- Le score d'exécution marketing de SentinelOne est impacté par ses faible notoriété de la marque , par rapport avec autres dirigeants.
- SentinelOne's capacité à prendre en charge sur place déploiements et systèmes qui ne sont pas directement connecté à Internet est partiel. En revanche , il des offres pleinement prise en charge des systèmes orientés vers le cloud .
- Produit XDR de SentinelOne est toujours évolution , par rapport aux solutions concurrentes d' autres vendeurs évalués dans ce Magic Quadrant.
- SentinelOne's clients serait accueillir Plus profond intégrations avec les solutions de sécurité réseau des principales appliances réseau vendeurs . Ces serait fournir une confiance zéro et un maillage de services opportunités et attirer les clients qui vouloir tirer le meilleur parti de l' existant investissements .

Sophos

Sophos est un leader dans ce Magic Quadrant.
Sophos a continué à développer son offre Adaptive Cybersecurity Plateforme Écosystème (ACE), avec trois acquisitions importantes en 2021 et 2022 qui conjointement améliorer la prise en charge de Linux, l'automatisation et les intégrations pour XDR, et la visibilité dans l'hébergement cloud environnements .
Sophos a également abordé la croissance besoin de services gérés flexibles et menace options de réponse - ce sont maintenant parmi les plus parties réussies de son portefeuille. La plate-forme ACE comprend les deux point final sécurité et sécurité du réseau fonctionnalités , ainsi que toutes les sécurités opérations outils nécessaires pour les intégrer et les gérer .
Les clients de Sophos sont principalement des organisations de type A et de type B , mais les organisations de type C sans le personnel de sécurité est également pris en charge via entièrement géré services de détection et de réponse aux incidents .
Forces

- Sophos obtient d'excellents résultats en matière de stratégie marketing exposant d'une plate-forme XDR complète. Il obtient également de bons résultats pour l' étendue de son portefeuille, qui inclut les outils de gestion , le réseau et les terminaux sécurité produits et prise en charge des charges de travail cloud .
- Sophos propose un service MDR. Les services tiers sont également disponible auprès des partenaires MSSP . De plus , Sophos a lancé une évaluation des compromis à coût fixe outil en juillet 2022.
- En 2022, Sophos a ajouté l'intégration avec l'API de sécurité Microsoft Graph. Il a aussi étendu c'est intégrations avec sécurité tierce _ outils et axés sur l'apport des gains d'efficacité à ses agent de point final .
- Sophos fournit une fonction de restauration utile pour la protection contre les rançongiciels courants et les logiciels malveillants associés .

Précautions

- Le score le plus bas de Sophos concerne l'exécution marketing . Son approche conservatrice du marketing ne génère pas assez d' occasions de concourir effectivement contre les autres Leaders de ce Magic Quadrant.
- Sophos manque d'options de déploiement sur site et de cloud privé , et est donc inapproprié pour les organisations avec ces exigences.
- Offres Sophos l'intégration entre outils tiers et son offre MDR mais manque _ l'intégration de ses données de votre propre produit mobile . Il a également n'a pas la capacité de gérer de manière intégrée produits tiers . _
- Sophos avait décevant résultats des évaluations MITRE ATT&CK Phase 4 du premier trimestre 2022, comparés avec celles des autres Leaders. Il avait important nombre de ratés et télémétrie détections ce analyse d' expert requise pour détecter les activité .

Treillix

Treillix est un acteur de niche dans ce Magic Quadrant. Treillix est une nouvelle entreprise formé autour des produits combinés de McAfee Enterprise et FireEye . Treillix essayant d' établir sa marque en tant que concurrent majeur dans le point final sécurité marché en entreprenant de vastes campagnes de marketing . Les produits combinés de McAfee Enterprise et FireEye sont volumineux, mais affichent des chevauchements qui n'ont pas encore été résolus . Treillix propose actuellement deux offres EDR , à savoir les anciennes offres MVISION et Helix , qui sont toutes deux des agents et des consoles de gestion distincts .
de Trellix les produits conviennent aux organisations mondiales de type B et C qui sont préparés pour le produit intégration et consolidation.
Forces

- Trellix obtient de bons résultats pour les attributs tels que les opérations et la viabilité , en raison de la profondeur et de l'étendue de son entreprise combinée capacités , ses géographique portée , et sa base installée mature de clients fidèles .
- de Trellix pour l'intégralité de la vision sont améliorés par son large gamme de sécurité produits et outils pour les systèmes hérités , ainsi que ses amélioration de la capacité EDR avec la combinaison des approches FireEye et McAfee Enterprise .
- Trellix continue de prendre en charge la sécurité réseau de FireEye appliances et outils SIEM/SOAR pour les clients qui y ont investi et qui souhaitent conserver _ eux .
- Treillix est bon pour soutenir clients qui ont investi dans la large gamme de solutions McAfee Enterprise technologie et sont familiers avec ses outils de gestion .

Précautions

- de Trellix Le score de complétude de la vision est retenu par l' exécution risque représentée par la consolidation des deux produits EDR en un seul agent et une seule console de gestion avec une conception d'interface utilisateur cohérente.
- Treillix reçoit un score faible pour l'exécution marketing car il travaille à remplacer deux marques bien connues avec une nouvelle marque inconnue .
- Treillis propose une feuille de route qui comprend poursuite de la consolidation et de la rationalisation de ses produits , mais la combinaison actuelle de fonctionnalités EDR réparties sur deux offres distinctes continue de confondre les acheteurs .
- Bien que Trelix a un accord de trois ans avec Google (Mandiant) pour fournir des services MDR tout en il se développe c'est propres capacités natives , Google est en concurrence avec Trélix quand il vient aux capacités XDR/SIEM .

Trend Micro

Trend Micro est un leader dans ce Magic Quadrant.
Trend Micro a récemment consolidé son cloud, son serveur et son endpoint solutions de sécurité , et a élargi sa marque Vision One XDR. Trend Micro prend en charge les versions hybrides sur site /cloud et cloud pur de son offre Vision One . L' entreprise a fait migrer ses existant clients vers les produits cloud une initiative majeure. Il offre support riche dans ses produits EPP et EDR pour un large catalogue des plates-formes actuelles et héritées .
Trend Micro était au début de l'établissement sa plate-forme XDR complète, qui il s'est élargi en utilisant une variété de SOAR, de gestion des services informatiques et de sécurité réseau améliorations et intégrations sur la plate-forme Trend One et des outils tiers . Il a une présence mondiale .
Forces

- Trend Micro obtient de très bons résultats fortement pour l' étendue de ses offrande et le fait que , ainsi que les plates-formes EDR et XDR de base , il fournit contrôle des appareils et des applications , prise en charge des systèmes de contrôle mobiles et industriels , DLP, stockage la sécurité et les services de sandboxing du réseau hébergé .
- Trend Micro prend en charge un large éventail de variantes de Linux et de plates-formes de serveur héritées . De plus , il maintient l'intégration avec c'est TXOne coentreprise , qui met l'accent sur la protection opérationnel technologie et terminaux IoT .
- Trend Micro a lancé une offre de gestion de surface d'attaque axée sur l'identification et la contribution les données sur les risques de surface d'attaque au niveau de l'organisation quantifié risque tableau de bord .
- Trend Micro obtient d'excellents résultats dans l'ensemble viabilité . Ceci publiquement négociés société , cotée à la Bourse de Tokyo, a une portée mondiale , une clientèle cohérente et soutenue performances financières .

Précautions

- Trend Micro marché le score de réactivité reflète c'est relativement petit part du marché global de l'EDR et des transactions pour plus de 500 postes .
- Bien que Trend Micro ait donné la priorité l'efficacité de son agent, avec des améliorations majeures de la taille et de l'empreinte mémoire , l'agent reste plus grand que d'autres , en raison de sa vaste catalogue de support de plate-forme.
- Bien que Trend Micro offre une gestion complète de ses produits via une offre MDR , cela est utilisé par seulement une minorité des employés de l'entreprise existant clients .
- Intégration XDR de Trend Micro est le plus riche parmi c'est posséder produits — la société n'a qu'un nombre modeste d' intégrations tierces .

VMware

VMware est un visionnaire dans ce Magic Quadrant.
Le point de terminaison VMware Carbon Black offre des capacités EPP et EDR et des services MDR à travers PC , serveurs et charges de travail cloud . En 2022, VMware a investi dans le déploiement d'une offre MDR fournie par VMware et l'introduction du Contexa produit de renseignements sur les menaces . Contexa combine les données de sécurité du réseau et de la messagerie avec point final télémétrie à partir d'autres dispositifs de sécurité VMware outils de vulnérabilité et de risque évaluation avec automatique remédiation .
Les produits VMware conviennent aux organisations de type A et de type B , en particulier ceux qui ont investi dans VMware vSphere et VMware NSX.
Broadcom a annoncé son intention d' acquérir l' encours parts de VMware, mais, au moment de l'évaluation , les deux Broadcom (Symantec) et VMware ont rempli les critères d'inclusion de ce Magic Quadrant et ont continué à fonctionner séparément .
Gartner va fournir un aperçu supplémentaire comme plus de détails devient disponible sur la future feuille de route pour ces portefeuilles existants des fournisseurs .
Forces

- VMware XDR optimisé par Contexa fournit l'intégration , la qualification et la corrélation des renseignements sur les menaces à partir de plusieurs outils VMware et tiers , et une plate-forme d' automatisation réponse et remédiation .
- En 2022, VMware a introduit une offre MDR directe , qui il s'est élargi avec automatique confinement .
- VMware obtient des scores très fortement pour les opérations , étant donné son vaste réseau et son marché pénétration .
- Améliorations de VMware Carbon Black Cloud inclure l'intégration de ses données dans ServiceNow sécurité outils et intégration avec Point de preuve pour l'identification, l'ingestion et le produit croisé remédiation des menaces par e-mail .

Précautions

- VMware reçoit un ci-dessous note moyenne pour le marché réactivité , grâce à sa faible marché part relative à l' exécution potentiel de son canal de vente
- VMware la note du produit est impacté par une baisse score global aux tests MITRE ATT&CK WizardSpider+Sandworm 2022 par rapport aux concurrents dans ce analyse .
- Le score d'innovation de VMware est limité par le rythme auquel il introduit de nouvelles fonctionnalités .
- L'impact de l' acquisition de Broadcom sur VMware des produits ne peut pas encore être déterminé , mais nous conseiller les clients poursuivant pluriannuel des investissements pour augmenter leur diligence.

WhitSecure

WhitSecure est un acteur de niche dans ce Magic Quadrant.
WithSecure est une nouvelle entreprise ce était formé en juin 2022 lorsque F- Secure d'entreprise l'activité de sécurité était dissociée des activités grand public de F-Secure et renommée . C’est une société finlandaise cotée en bourse. WithSecure fournit des fonctionnalités EPP et EDR natives du cloud, ainsi que la protection des e-mails, de la collaboration pour Microsoft Office 365 et la gestion des vulnérabilités . withSecure Contrecept fournit des services MDR.
La plupart de WithSecure les clients se trouvent dans la région EMEA, en Asie/Pacifique et au Japon. WhitSecure Éléments offre est approprié pour les organisations de type B et de type C à ressources limitées.
Forces

- WhitSecure's le score du produit reflète récent améliorations , y compris un scanner de mémoire pour le déploiement lors d'un incident, actions de réponse EDR enchaînées et notifications proactives de l'administrateur en cas de mauvaise configuration points de terminaison .
- Une fonctionnalité EPP premium appelé DataGuard fournit basé sur des politiques le cantonnement des fichiers ou dossiers attribués en tant que couche supplémentaire de protection contre les ransomwares.
- WhitSecure propose un service MDR conforme au Règlement général sur la protection des données (RGPD) pour les clients de l'UE .
- WhitSecure Capacité EDR des éléments est facile à configurer et à utiliser. De plus , il a une option unique pour élever alertes directement depuis la console vers WithSecure chasseurs de menaces , qui offrir deux heures temps de réponse .

Précautions

- de WithSecure pour servir plus de principalement taille moyenne les entreprises ont obtenu des résultats mitigés . Le rebranding de l' entreprise et de ses offrandes pourrait ralentir sa croissance dans de nouveaux domaines.
- La solution XDR de WithSecure est immature et, prête à l'emploi, intègre avec uniquement Microsoft Office 365. WithSecure's le portefeuille de produits manque de solutions de sécurité des données , de réseau, SSE et SEG.
- la capacité EDR de WhitSecure ne s'étend pas à la détection personnalisée règles ou playbooks . Menace chasse est limité , et là n'est pas capable d' intégrer avec externe menace se nourrit .
- WithSecure a réalisé bien dans les tests effectués par AV-TEST, mais ses résultats de test MITRE ATT&CK Round 4 révéler des lacunes dans les deux analytique couverture et nombre de détections , en comparaison avec des Leaders dans ce Magic Quadrant.

Fournisseurs ajoutés et supprimés

Nous devons revoir et ajuster nos critères d'inclusion pour les Magic Quadrants à mesure que les marchés évoluent. A la suite de ces , la combinaison de fournisseurs dans un Magic Quadrant peut changer au fil du temps. Un vendeur apparition dans un Magic Quadrant une année et pas l' autre n'est pas nécessairement indiquer ce nous avons changé notre avis là-dessus vendeur . Il peut être le reflet d'une évolution du marché et, par conséquent , modifié évaluation critères , ou d' un changement d' orientation par ce vendeur .

Ajoutée

- Instinct profond
- Réseaux de Palo Alto
- Treillis

Abandonné

- FireEye (voir Treillis)
- F-Secure (remplacé par WithSecure)
- McAfee (voir Treillis)
- Sécurité Panda